(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2001 (31.05.2001)

PCT

(10) International Publication Number
WO 01/39121 A1

(51) International Patent Classification[7]: G06T 1/00, H04N 1/32, 5/913

(21) International Application Number: PCT/EP00/10729

(22) International Filing Date: 30 October 2000 (30.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
99203914.9 23 November 1999 (23.11.1999) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: DEPOVERE, Geert, F., G.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). KALKER, Antonius, A., C., M.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). EVELEENS, Jan; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: SCHMITZ, Herman, J., R.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

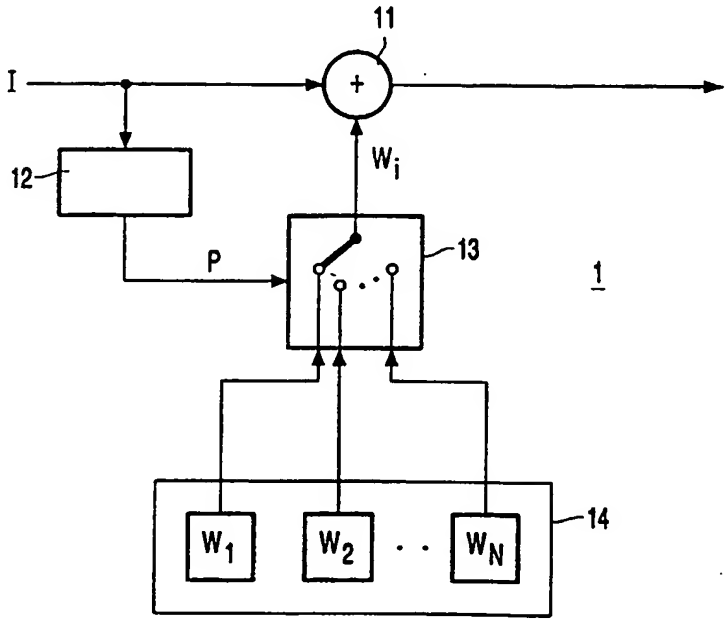
(81) Designated States *(national)*: CN, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: WATERMARK EMBEDDING AND DETECTION



(57) Abstract: A method and arrangement for embedding and detecting a watermark in an information signal is disclosed. The embedded watermark (W_i) is selected (13) from a plurality of watermarks ($W_1..W_N$) in dependence upon a property P of the signal. An example of such a property is the distribution of luminance values of the current video image as calculated by an analysis circuit (12). The corresponding watermark detector performs the same operation: the watermark being looked for depends on the same signal property. It is achieved with the invention that the embedded watermark changes from time to time as a function of the information signal content, so that it cannot easily be hacked.

WO 01/39121 A1

Watermark embedding and detection.

FIELD OF THE INVENTION

The invention relates to a method and arrangement for watermarking an information signal, for example, an audio or video signal. The invention also relates to a method and arrangement for detecting a watermark in such an information signal.

BACKGROUND OF THE INVENTION

A known method of watermarking a video signal is disclosed in International Patent Application WO-A-99/45705. In this method, a watermark pattern is added to the video signal. A watermark detector correlates the same pattern with the suspect signal. If the correlation exceeds a given threshold, the pattern is said to be present. The presence or absence of the pattern represents a single bit of information. The embedded watermark may also carry a multi-bit payload. In the system disclosed in WO-A-99/45705, the payload is represented by a combination of one or more basic patterns and spatially shifted versions thereof. The payload is encoded into the respective shift vectors. The watermark detector correlates each basic pattern with the suspect signal, and determines the spatial positions of the basic patterns with respect to each other. The detector further checks whether said positions constitute a valid payload.

The process of correlating watermark patterns with the suspect signal requires the watermark detector to have locally stored versions of said patterns. In view thereof, it is desired that the watermarking system employs only a few different patterns. The patterns being used are kept secret to the outside world. However, even without knowledge of the patterns, a hacker can compromise the system if he has the relevant embedder at his disposal. He may feed an arbitrary input signal to said embedder and subtract the signal from its watermarked version. The difference signal thus obtained resembles the watermark of any other watermarked signal, depending on the perception model used in the watermark embedder at hand. If the difference signal is combined with (e.g. added to or subtracted from) a watermarked signal, the embedded watermark will substantially be cancelled or at least no longer represent a valid payload. In either case, the embedded watermark has been made ineffective.

OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a more secure method and arrangement for embedding and detecting a watermark in an information signal, even if a hacker has a watermark embedder at his disposal.

To this end, the method in accordance with the invention comprises the steps of analyzing a given property of the information signal and determining an actual value of said property, associating different watermarks with distinct values of said property, and embedding the watermark associated with said actual value. The corresponding watermark detection method comprises the steps of analyzing a given property of the information signal and determining an actual value of said property, associating different watermarks with distinct values of said property, and detecting the watermark associated with said actual value.

It is achieved with the invention that the embedded watermark pattern changes from time to time, as a function of the information signal content. Feeding an arbitrary signal to an embedder so as to produce a signal that resembles the watermark, as described above, does not work anymore because the arbitrary signal has different properties. A significant advantage of the invention is that the number of different watermark patterns which the detector must store can be kept much lower. Said number is a result of balancing detector complexity versus security.

There are numerous examples of properties of the information signal that can be used for selecting the watermark pattern to be embedded. The only requirement to be fulfilled is its robustness or invariance with respect to the embedded watermark. Advantageous examples of properties are distinct distributions of luminance values of a video signal, or distinct shapes of the frequency spectrum of an audio signal.

Further aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter. The examples relate to watermark embedding and detection of video signals, but it will be appreciated that the invention equally applies to audio signals or any other type of multimedia signal.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows schematically a diagram of a watermark embedder in accordance with the invention.

Fig. 2 shows schematically a diagram of a watermark detector in accordance with the invention.

Fig. 3 shows an arrangement to illustrate the operation of the watermark embedder and detector.

Figs. 4 and 5 show further embodiments of the watermark embedder in accordance with the invention.

Fig. 6 shows a further embodiment of the watermark detector in accordance with the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 shows schematically a diagram of an embodiment of a watermark embedder **1** in accordance with the invention. It will here be assumed that the embedded watermark represents a 1-bit payload. For example, the absence of a watermark indicates that the video signal may freely be copied, whereas the presence of a predetermined watermark denotes that making a copy of the signal is prohibited.

The embedder receives an input video signal I in the form of a sequence of images, and comprises an adder **11** which adds a watermark pattern W_i to each image. The embedder further comprises an image analyzer **12**, a selector **13** and a read-only memory **14** in which a plurality of different watermark patterns $W_1..W_N$ are stored. The analyzer **12** receives the video signal and analyzes a given property P of the video signal as a function of time. The actual value of property P found by analyzer **12** is applied to the selector **13**. In response thereto, the selector selects one of the stored watermark patterns $W_1..W_N$ to the adder **11** for embedding.

The analyzer **12** may take numerous forms. A few examples will be given to provide sufficient teaching to enable a skilled person to design appropriate alternative embodiments. The property being analyzed may be the distribution of luminance values across the image (spatial distribution) or across a sequence of images (temporal distribution). In a first example, the analyzer divides each image into sub-images, and determines which of said sub-images has the highest average luminance. The relevant sub-image number is the actual value of property P. In a second example, the analyzer assigns a "0" to each sub-image having a low average luminance and a "1" to each sub-image having a high average luminance. Each video image is now characterized by an n-bit code, where n is the number of sub-images. The relevant n-bit code is the actual value of property P. The property being analyzed may also be local image activity. Such an analysis can easily be carried out in the frequency domain.

Fig. 2 shows schematically a diagram of a preferred embodiment of a watermark detector **2** in accordance with the invention. The detector receives a suspect video

signal J and comprises an image analyzer **22**, a selector **23** and a read-only memory **24** which are identical to the corresponding counterparts of embedder **1**. Accordingly, the analyzer **22** analyzes the same property P of the video signal, and the selector **23** selects the same watermark pattern W from the stored patterns $W_1..W_N$, as the embedder.

The detector further comprises a correlation circuit **21** which calculates the correlation between each image of the suspect video signal and the applied watermark pattern W_i. If the correlation exceeds a predetermined threshold, the selected watermark pattern W_i is said to be present (D=1), otherwise it is said to be absent (D=0).

The correlation circuit **21** is preferably of a type which performs the correlation for all possible spatial positions of the applied watermark with respect to the image. Such a correlation circuit is disclosed in WO-A-99/45705. It generates a correlation pattern which exhibits a peak for each spatial position of the watermark. WO-A-99/45705 describes that multiple peak positions may represent a payload. However, as mentioned above, the payload in this example is a 1-bit copy control signal. The detection circuit **2** will consider the presence of 2 or more peaks as an invalid payload (D=0).

It is assumed that the watermark patterns $W_1..W_N$ are secret and can neither be retrieved by interrogating the embedder or detector circuits. As will now be explained with reference to Fig. 3, the invention prevents a hacker from compromising the system when he happens to have an embedder at his disposal. In Fig. 3, a potential hacker receives a video signal V' being watermarked by an embedder **1a**. The signal V' may be a recorded signal, in which case the actual embedding took place a long time ago. The embedder **1a** is of a type as described above with reference to Fig. 1.

The hacker has an identical embedder **1b** at his disposal. An arbitrary video signal X is applied to said embedder **1b** so as to locally generate a watermarked video signal X'. An adder **3** subtracts the arbitrary signal X from its watermarked version X'. The difference signal (which strongly resembles the embedded watermark pattern) is then combined with (added to or subtracted from) the watermarked signal V' by a further adder **4**. The suspect signal V" thus processed is applied to a watermark detector **2** as described above with reference to Fig. 2.

Without the provisions of the invention, both embedders **1a** and **1b** embed the same watermark in the respective input signals. This results either in a cancellation of the watermark in the suspect signal V" or in an invalid payload due to multiple occurrences of the watermark pattern W at different positions. In both cases, the detector generates an output signal D=0 and the hacking attack is successful.

With the provisions of the invention, the watermark W_i (i=1..N) in signal V' will generally differ from the watermark W_j (j=1..N) in signal X', because the contents of the original video signals V and X are different. The property analysis algorithm of detector **2** responds to the contents of signal V" which is substantially equal to the contents of V. Consequently, the watermark pattern being checked by detector **2** is the watermark pattern W_i which has been embedded by embedder **1a**. The detector ignores the additional presence of a different pattern W_j, and the hacking attack thus fails.

A possible work-around is feeding the watermarked signal V' instead of an arbitrary signal X to embedder **1b**, so as to force embedder **1b** to select the same watermark W_i as embedder **1a**. To avoid this, the embedders **1a** and **1b** are preferably of a type that refrains from embedding a watermark in a signal that has already been watermarked. Fig. 4 shows a schematic diagram of such an embedder. It comprises the same adder **11**, image analyzer **12**, selector **13** and ROM **14** as the embedder which is shown in Fig. 1. It further comprises the correlation circuit **21** of the detector which is shown in Fig. 2. The correlation circuit **21** detects whether the input signal I already includes the watermark pattern W_i to be embedded. If that is the case (D=1), a switch 15 is controlled to prevent the watermark pattern W_i from being embedded multiple times.

Fig. 5 shows a schematic diagram of a watermark embedder for embedding multi-bit payload in the video signal. The embedder comprises the same adder **11**, image analyzer **12**, selector **13** and ROM **14** as described before with reference to Fig. 1. The ROM **14** now stores a plurality of sets of watermark patterns. The embedder further includes an encoding circuit **16** which receives a selected set i of basic watermark patterns $W_{i,1}$, $W_{i,2}$, ..., and encodes a multi-bit payload d into the relative positions of said patterns. The basic patterns have a relatively small size (e.g. 128×128 pixels). The watermark pattern generated by encoder **16** is subsequently tiled over the image by a tiling circuit **17**. The ROM **14** stores different sets of basic patterns for different values of signal property P. The actual set of basic patterns being applied to encoder **16** is controlled by the actual value of property P and changes as a function of time.

Fig. 6 shows the corresponding watermark detector. The detector comprises a folding circuit **25** for folding and storing image segments of 128×128 pixels in a buffer prior to correlation. The detector further comprises the same correlation circuit **21**, image analyzer **22**, selector **23** and read only memory **24** as described before with reference to Fig. 2. The ROM **24** stores different sets of basic patterns for different values of signal property P. The

actual set of basic patterns being applied to the correlation circuit **21** is controlled by the actual value of property P.

It should be noted that the invention is not limited to the watermarking systems described in the embodiments. For example, a watermarking system is known that uses n different watermark patterns, each pattern corresponding to one bit of an n-bit payload. In accordance with this invention, the embedder and detector of such a system include different sets of n patterns. A particular set is then selected in response to the actual value of a signal property.

In summary, a method and arrangement for embedding and detecting a watermark in an information signal is disclosed. The embedded watermark (W_i) is selected (13) from a plurality of watermarks ($W_1..W_N$) in dependence upon a property P of the signal. An example of such a property is the distribution of luminance values of the current video image as calculated by an analysis circuit (12). The corresponding watermark detector performs the same operation: the watermark being looked for depends on the same signal property. It is achieved with the invention that the embedded watermark changes from time to time as a function of the information signal content, so that it cannot easily be hacked.

CLAIMS:

1. A method of embedding a watermark in an information signal, comprising the steps of:

- analyzing a given property of the information signal and determining an actual value of said property;
- associating different watermarks with distinct values of said property; and
- selecting the watermark associated with said actual value for embedding in the information signal.

2. A method as claimed in claim 1, in which the information signal is a sequence of video images, said analyzing step comprising analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.

3. A method as claimed in claim 1, in which the information signal is a sequence of audio signal segments, said analyzing step comprising analyzing a shape of the frequency spectrum of said audio segments, each distinct shape of the frequency spectrum constituting a value of said property of the information signal.

4. A method as claimed in claim 1, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of the property of the information signal.

5. A method of detecting a watermark in an information signal, comprising the steps of:

- analyzing a given property of the information signal and determining an actual value of said property;
- associating different watermarks with distinct values of said property; and
- selecting and detecting the watermark associated with said actual value.

6. A method as claimed in claim 5, in which the information signal is a sequence of video images, said analyzing step comprising analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.

7. method as claimed in claim 5, in which the information signal is a sequence of audio signal segments, the method comprising the steps of calculating the frequency spectrum for each segment, each distinct shape of said frequency spectrum constituting a value of said property of the information signal.

8. method as claimed in claim 5, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of the property of the information signal.

9. watermark embedder for embedding a watermark in an information signal, comprising:

- means (12) for analyzing a given property (P) of the information signal and determining an actual value of said property;
- means (14) for associating different watermarks with distinct values of said property; and
- means (13) for selecting the watermark associated with said actual value for embedding (11) in the information signal.

10. A watermark detector for detecting a watermark in an information signal, comprising:

- means (22) for analyzing a given property of the information signal and determining an actual value of said property;
- means (24) for associating different watermarks with distinct values of said property; and
- means for selecting (23) and detecting (21) the watermark associated with said actual value.

11. A watermark embedder as claimed in claim 9, further including a watermark detector as claimed in claim 10, and comprising means (15) for refraining from embedding the

selected watermark in response to said detector detecting said selected watermark in the information signal.

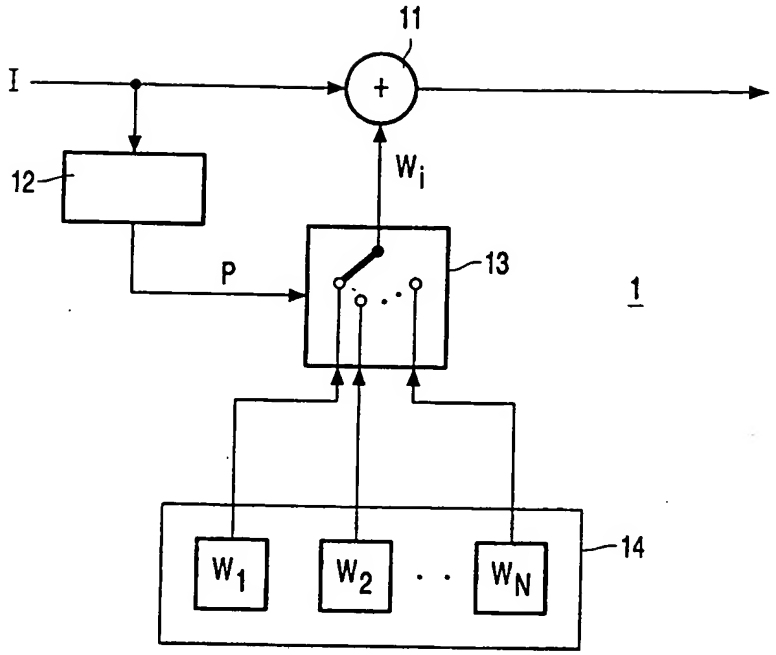


FIG. 1

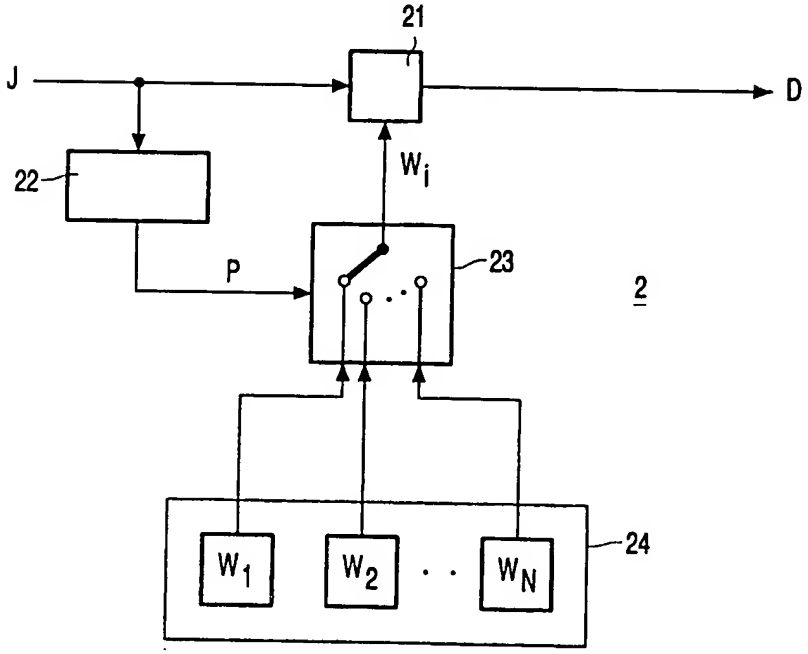


FIG. 2

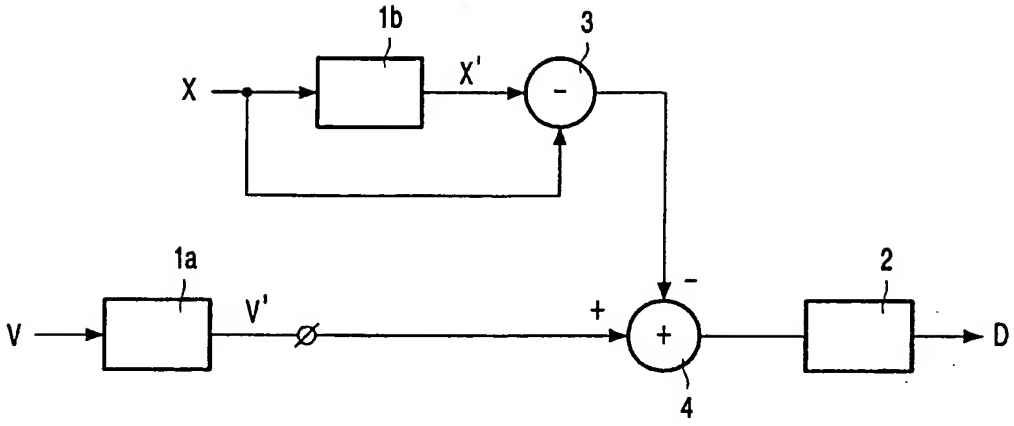


FIG. 3

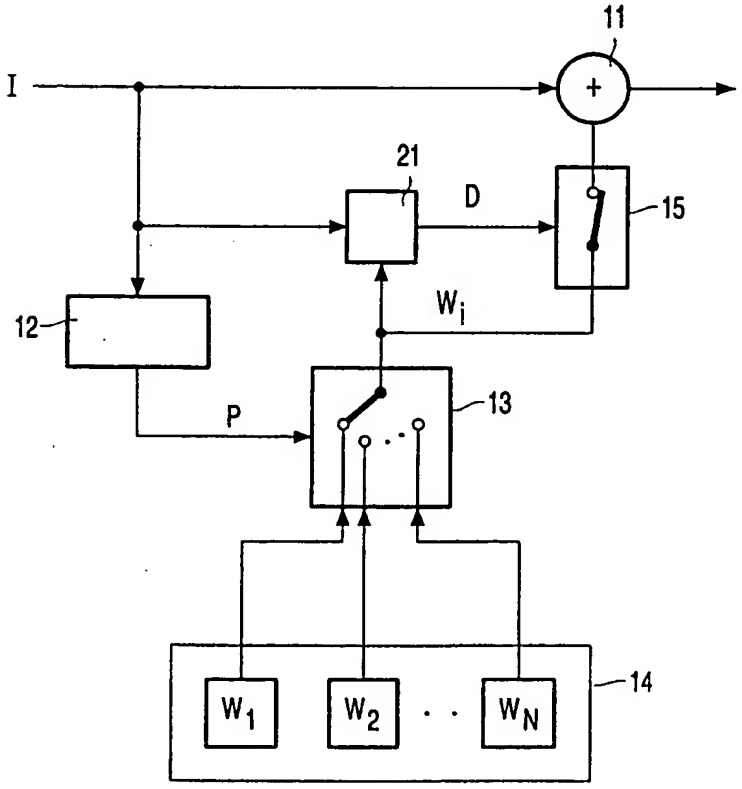


FIG. 4

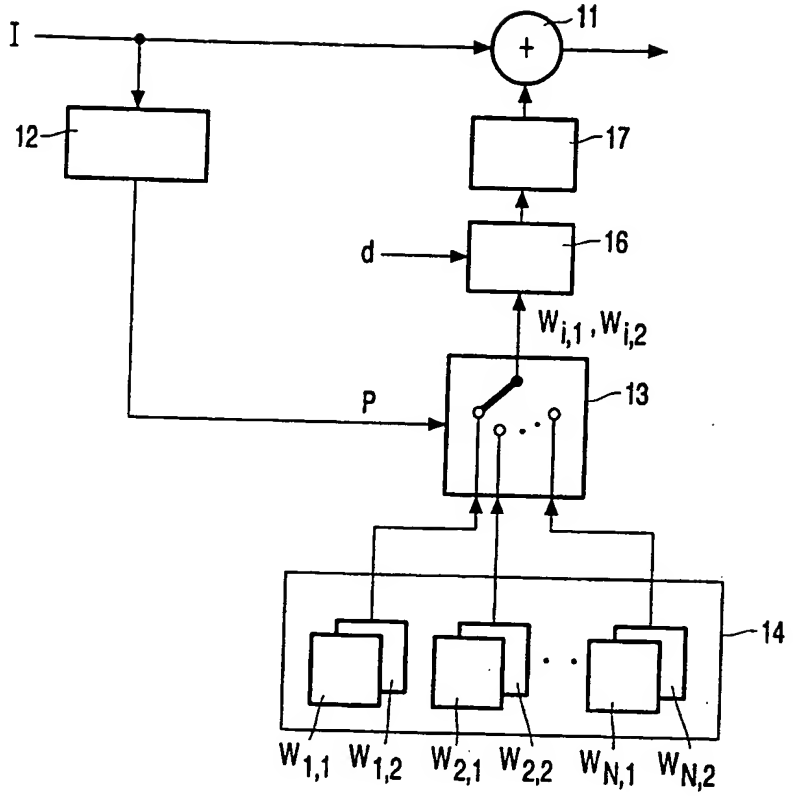

I
11
+
12
17
d
16
$W_{i,1}, W_{i,2}$
P
13
14
$W_{1,1}$ $W_{1,2}$ $W_{2,1}$ $W_{2,2}$ $W_{N,1}$ $W_{N,2}$

FIG. 5

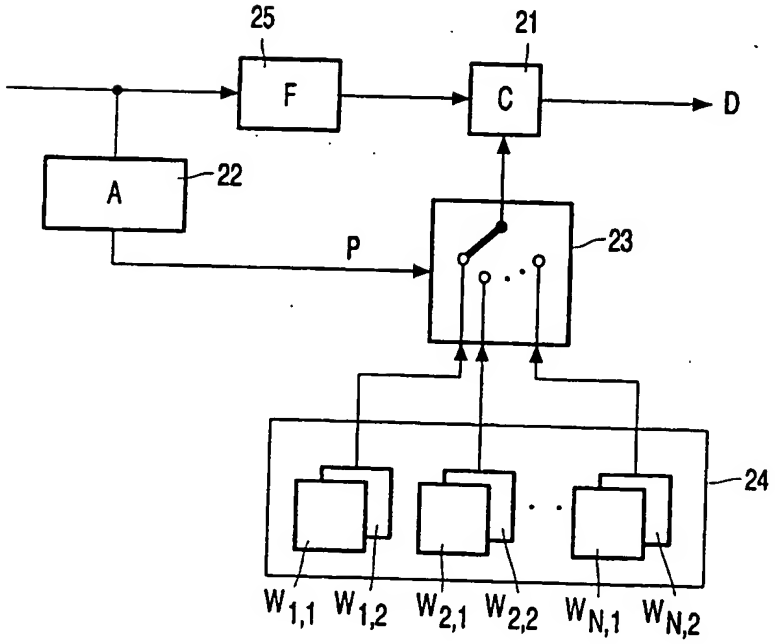

25
21
F
C
D
A
22
P
23
24
$W_{1,1}$ $W_{1,2}$ $W_{2,1}$ $W_{2,2}$ $W_{N,1}$ $W_{N,2}$

FIG. 6

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/EP 00/10729

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06T1/00 H04N1/32 H04N5/913

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06T H04N H04H G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HANGSHENG XU ET AL: "Applications of digital watermarking technology in audio signals" J. AUDIO ENG. SOC, JOURNAL OF THE AUDIO ENGINEERING SOCIETY, vol. 47, no. 10, October 1999 (1999-10), pages 805-812, XP000928475 USA	1,3,4,9
A	paragraph '03.1! - paragraph '03.3! ---	5,7,8,10
X	EP 0 860 997 A (NIPPON ELECTRIC CO) 26 August 1998 (1998-08-26) figures 1,5,7,8,10 column 7, line 19 -column 8, line 36 column 9, line 23 - line 42	1,5,9,10
A	column 10, line 24 -column 11, line 32 --- -/--	2,6,11

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 January 2001	12/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 00/10729

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 326 556 A (NIPPON ELECTRIC CO) 23 December 1998 (1998-12-23) figure 1 page 7, line 26 -page 8, line 27	1,9
A	page 11, line 4 - line 19	2
A	DITTMANN J ET AL: "Content-based digital signature for motion pictures authentication and content-fragile watermarking " PROCEEDINGS OF ICMCS99: IEEE INTERNATIONAL CONFERENCE ON MULTIMEDIA COMPUTING AND SYSTEMS, vol. 2, 7 - 11 June 1999, pages 209-213, XP002158357 Florence, Italy the whole document	1,2,5,6, 9,10
E	WO 00 72321 A (MICROSOFT CORP) 30 November 2000 (2000-11-30) abstract	1,3,9

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

..formation on patent family members

Inter ›nal Application No
PCT/EP 00/10729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0860997 A	26-08-1998	CA 2230183 A	24-08-1998
		JP 11055639 A	26-02-1999
GB 2326556 A	23-12-1998	JP 11008753 A	12-01-1999
WO 0072321 A	30-11-2000	NONE	